UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/827,469	04/06/2001	Chris Russell	041892-0203	6154

34492 7590 03/24/2005

SIDLEY AUSTIN BROWN & WOOD LLP (LAIP GROUP)
555 W. FIFTH ST., SUITE 4000
LOS ANGELES, CA 90013

EXAMINER	
BACKER, FIRMIN	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/827,469	RUSSELL ET AL.	
	Examiner	Art Unit	
	Firmin Backer	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Amendment

1. This is in response to an amendment file on January 6th, 2005. In the amendment, claims 1, 2, 11, 17, 21, 30 and 37 have been amended, no claim has been canceled, and no claim has been added. Claims 1-49 remain pending in the letter.

Response to Arguments

2. Applicant's arguments with respect to claims 1-49 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leonard et al (*U.S. PG Pub 2002/0052933*) in view of Yamaguchi et al. (*U.S. Patent No 5,323,244*) in further view of Bernadeau (*U.S. Patent No. 6,813,709).*

5. As per claims 1, 17, 21 and 37, Leonard et al teach a system for secure licensing of content to a user on a user network-enabled device (*see fig 1)*, comprising at least one server network device (*server 104)* communicatively coupled to the user network-enabled device (*client 100)* wherein the at least one server network device is programmed to transfer (*transfer/communicate)* selected content (*music content, sound content, image content, movie*

content, other content, 200, fig 2) to the user network-enabled device (*see paragraphs* and a license generator (*304)* , the license generator being programmed to generate a license (*offer license, 304)* associated with the selected content (*media license, 300)*, the license comprising access information for controlling the user network-enabled device to produce a user-perceptible form of the selected content when conditions defined by the access information are met (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423)*. Leonard et al fail to teach an inventive concept of inhibiting production of a user-perceptible form of the selected content when conditions defined by the access information are not met. However, Yamaguchi et al teach an inventive concept of inhibiting production of a user-perceptible form of the selected content when conditions defined by the access information are not met (*see column 1 lines 27-34, 4 lines 59-5 line 16, 5 line 44-6 line 13)*. Therefore it would have been obvious to one of ordinary skill in the art at the invention was made to modify the inventive concept of Leonard et al to include Yamaguchi et al's inventive concept of inhibiting production of a user-perceptible form of the selected content when conditions defined by the access information are not met because this would have ensure that only the authorized user with specified access right can access the content for reproduction. The combination of Leonard et al and Yamaguchi et al fail to teach an inventive concept wherein a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content. However, Bernadeau teaches an inventive concept wherein a root key for decrypting the encrypted license to allow the access information and the encryption key in the

encrypted license to be accessed by the media player and security technology the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content (*see abstract, column 1 lines 66- line 34 and claims 1 and 15).* Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined inventive concept of Leonard et al and Yamaguchi et al to include Bernadeau's inventive concept wherein a root key for decrypting the encrypted license to allow the access information and the encryption key in the encrypted license to be accessed by the media player and security technology the media player and security technology controlling a specific media player on the user network-enabled device to produce the user-perceptible form of the selected encrypted content because this would provide added security to the system.

6. As per claims 2, Leonard et al teach a system wherein the at least one server network device is further programmed to receive at a first node on the network a request for content from the user network-enabled device at a second node on the network; wherein the transfer of selected content comprises transferring the requested content in response to the receipt of the request at the second node (*see fig 1).*

7. As per claims 3, Yamaguchi et al teach a system wherein the content is encrypted (*see abstract, fig 1, 2).*

8. As per claims 4, Leonard et al teach a system wherein the at least one server network device is further programmed to receive at the first node on the network a request for the license from the user network-enabled device at the second node on the network; and wherein the at least one server network device is further programmed to transfer the requested license to the user network-enabled device at the second node (*see paragraphs 0273-0327, 0422, 0423).*

9. As per claims 5, 18, Leonard et al teach a system wherein the license is a data object (*see paragraphs 0273-0327, 0422, 0423).*

10. As per claims 6, 19, Leonard et al teach a system wherein the data object comprises a plurality of data fields, at least a portion of the plurality of data fields containing the access information (*see paragraphs 0273-0327, 0422, 0423).*

11. As per claims 7, 20, Yamaguchi et al teach a system wherein the access information comprises at least one of a content rental model, an expiration date of the license, user network-enabled device identification information, media player identification information, a GUID identifying particular content, and an encryption key for decrypting encrypted content (*see abstract, fig 1, 2).*

12. As per claims 8, Leonard et al teach a system wherein the content rental model defines at least one of a specified period of time and a specified number of plays (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423).*

13. As per claims 9, Leonard et al teach a system wherein the content rental model defines an unlimited number of plays on any user network-enabled device (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423)*.

14. As per claims 10, Leonard et al teach a system wherein the content rental model includes a watermark, the watermark allowing the user to rewind only a determined time interval from the current position in the movie ((*see paragraphs 0273-0327, 0422, 0423)*.

15. As per claims 11, Leonard et al teach a system further comprising at least one application server, the at least one application server being communicatively coupled to both the at least one server network device and the license generator; wherein the at least one application server is programmed to receive the license request from the at least one server network and to transfer the license request to the license generator (*see paragraphs 0273-0327, 0422, 0423)*.

16. As per claims 12, Leonard et al teach a system wherein the at least one application server is further programmed to provide business rules to the license generator, the business rules being included in the license request by the at least one application server before transferring the license request to the license generator, the business rules defining the types of licenses that the license generator may generate (*see paragraphs 0273-0327, 0422, 0423)*.

17. As per claims 13, Leonard et al teach a system wherein the at least one application server is further programmed to gather and store personalization information about users (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423).*

18. As per claims 14, Leonard et al teach a system wherein the at least one application server is further programmed to create dynamic Web pages (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423).*

19. As per claims 15, Leonard et al teach a system further comprising a firewall situated between the at least one server network device and the at least one application server, the firewall preventing unauthorized access to the at least one application server (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423).*

20. As per claims 16, Leonard et al teach a system further comprising a firewall situated between the at least one application server and the license generator, the firewall preventing unauthorized access to the license generator (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423).*

21. As per claims 22, 38, Leonard et al teach a system wherein the media player and security technology comprises a media player for displaying the content in a user-perceptible form (*see figs 29-36).*

22. As per claims 23, 39, Yamaguchi et al teach a system wherein the media player and security technology further comprises at least one of decryption code for decrypting encrypted content, a CODEC for decompressing compressed content, a monitor for displaying the media player to the user, and a hardware interface between the media player and the monitor (*see figs 1, 2).*

23. As per claims 24, 40, Yamaguchi et al teach a system wherein the media player and security technology further comprises digital rights management code for providing a secure inter-process communication data stream between the decryption code, the CODEC, the media player, the hardware interface, and the monitor (*see column 1 lines 27-34, 4 lines 59-5 line 16, 5 line 44-6 line 13).*

24. As per claims 25, Yamaguchi et al teach a system wherein the digital rights management code is protected against tampering by at least one of code obfuscation and anti-debugging techniques (*see column 1 lines 27-34, 4 lines 59-5 line 16, 5 line 44-6 line 13).*

25. As per claims 26, Leonard et al teach a system wherein the digital rights management code provides the secure inter-process communication data stream between the decryption code, the CODEC, the media player, the hardware interface, and the monitor by performing an integrity check on at least one of the media player, the decryption code, the CODEC, the hardware interface, and the monitor in order to detect tampering (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423).*

26. As per claims 27, Leonard et al teach a system wherein the digital rights management code inhibits the display of content in a user-perceptible form when at least one of the media player, the decryption code, the CODEC, the hardware interface, and the monitor do not pass the integrity check (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423)*.

27. As per claims 28, Leonard et al teach a system wherein the media player and security technology further comprises a protected database in communication with the digital rights management code; wherein the protected database securely stores transferred licenses (*see paragraphs 0273-0327, 0422, 0423)*.

28. As per claims 29, 42, Yamaguchi et al teach a system wherein the protected database is protected by encryption methods (*see column 1 lines 27-34, 4 lines 59-5 line 16, 5 line 44-6 line 13)*.

29. As per claims 30, 43, Leonard et al teach a system wherein the digital rights management code comprises a root key, the root key unlocking licenses within the protected database (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423)*.

30. As per claims 31, 44, Leonard et al teach a system wherein the digital rights management code examines the access information within the unlocked license and determines the access

rights to the content provided by the unlocked license (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423).*

31. As per claims 32, 45, Leonard et al teach a system wherein the access information comprises at least one of a content rental model, an expiration date of the license, user network-enabled device identification information, media player identification information, a GUID identifying particular content, and an encryption key for decrypting encrypted content (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423).*

32. As per claims 33, 46, Leonard et al teach a system wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by enforcing compliance by the user with the content rental model contained in the unlocked license (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423).*

33. As per claims 34, 47, Leonard et al teach a system wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by comparing user network-enabled device identification information in the unlocked license with the user network-enabled device on which the digital rights management code resides (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423).*

34. As per claims 35, 48, Leonard et al teach a system wherein the digital rights management code allows the user network-enabled device to produce a user-perceptible form of the content only when the content is properly licensed by comparing media player identification information in the unlocked license with the media player on the user network-enabled device on which the digital rights management code resides (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423)*.

35. As per claims 36, 49, Leonard et al teach a system wherein the digital rights management code passes the encryption key contained in the unlocked license to the decryption code in order to decrypt the encrypted content (*see figs 29-36, paragraphs 0006, 0045, 0048, 0049, 0273-0327, 0422, 0423)*.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (*see form 892)*.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The examiner can normally be reached on Mon-Thu 9:00 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on (703) 305-9768. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firmin Backer
Primary Examiner
Art Unit 3621

March 18, 2005